Amendments to the Claims

1. (currently amended) A method for operating a public-key encryption scheme which provides for sending a digital message M between a sender and a recipient with participation of an authorizer, wherein the digital message is encrypted by the sender and decrypted by the recipient, the method comprising encrypting, by at least one machine in a set of one or more machines, the digital message M using at least a recipient public key RPUB and a recipient encryption key RENC to create an encrypted digital message for decryption with a recipient private key RPRIV and a recipient decryption key RDEC, wherein:

the recipient public key RPUB and the recipient private key RPRIV form a public key/ private key pair 1, wherein the recipient private key RPRIV is a secret of the recipient;

the recipient decryption key RDEC is generated using at least a key generation secret of the authorizer and the recipient encryption key RENC, wherein a key formed from the recipient encryption key RENC and a key formed from the recipient decryption key RDEC are a public key/ private key pair 2.

2. (currently amended) The method of claim 1, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient.

3. (currently amended) The method of claim 1, wherein the recipient encryption RENC key is generated from information comprising a parameter defining a validity period for the recipient decryption key RDEC.

4. (currently amended) The method of claim 1, wherein the recipient encryption key RENC is generated from information comprising the recipient public key RPUB.

5. (currently amended) The method of claim 1, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient, the recipient public key RPUB, and a parameter defining a validity period for the recipient decryption key RDEC.

6. (currently amended) The method of claim 1, wherein the recipient decryption key RDEC is generated by the authorizer according to a schedule known to the sender.

7. (currently amended) The method of claim 6, wherein the recipient encryption key RENC is generated using at least information comprising the schedule.

8. (currently amended) The method of claim 1, wherein the recipient private key RPRIV and the recipient public key RPUB are generated using at least one system parameter issued by the authorizer.

9. (currently amended) The method of claim 1, wherein the recipient decryption key RDEC is generated by the authorizer to have a value $S = s_c P_B$, wherein:

s_c is the key generation secret of the authorizer; and

P_B is the recipient encryption key RENC and is equal to $H_1(\text{Inf}_B)$, wherein Inf_B is an element of a first cyclic group $\mathbb{G}_1$ of elements, wherein P_B is an element of a second cyclic group $\mathbb{G}_2$ of elements, and H_1 is a predefined function ("first function H_1"), wherein the first and second cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ and the function H_1 are system parameters made available to the sender, and also available to the sender are system parameters comprising:

a generator P of the first cyclic group $\mathbb{G}_1$;

a key generation parameter $Q = s_C P$;

a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$.

10. (currently amended) The method of claim 9, wherein Inf_B comprises the identity of the recipient, ID_{rec}, the recipient public key RPUB, and a parameter defining a validity period for the recipient decryption key RDEC.

11. (Original) The method of claim 9, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

12. (Original) The method of claim 9 wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

13. (previously presented) The method of claim 9 wherein the system parameters available to the sender further comprise a function $\hat{e}$ which is a bilinear, non-degenerate, and efficiently computable pairing which maps $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$.

14. (previously presented) The method of claim 11 wherein:

s_C is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$.

15. (currently amended) The method of claim 9, wherein encrypting the digital message M comprises:

generating an element $P'_B = H_1(ID_{rec})$, wherein ID_{rec} comprises the identity of the recipient and wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

selecting a random key generation secret r; and

encrypting the digital message M to form a ciphertext C, wherein C is set to be:

$C = [rP, M \oplus H_2(g^r)]$, where $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, where PK_B is the recipient public key RPUB and wherein ê is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$.

16. (currently amended) The method of claim 1, wherein the recipient encryption key RENC is generated from a document and the recipient decryption key RDEC is the authorizer's signature on the document.

17. (currently amended) The method of claim 11, wherein encrypting the digital message M comprises:

generating an element $P'_B = H_1(ID_{rec})$ wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

choosing a random parameter $\sigma \in \{0,1\}^n$;

set a random key generation secret $r = H_3(\sigma, M)$; and

encrypting the digital message M to form a ciphertext C, wherein C is set to be:

$C = [rP, M \oplus H_2(g^r), E_{H_4(\sigma)}(M)]$, where $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, wherein PK_B is the recipient public key RPUB, wherein H_3 is a function capable of generating an

integer of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ from two strings of binary digits, H_4 is a function capable of generating one binary string from another binary string, E is a symmetric encryption scheme, ê is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$, and $H_4(\sigma)$ is the key used with E.

18. (currently amended) A method for operating a public-key encryption scheme which provides for sending a digital message between a sender and a recipient with participation of a plurality of authorizers, the plurality of authorizers including a root authorizer and *n* lower-level authorizers in a hierarchy between the root authorizer and the recipient, wherein $n \geq 1$, the method comprising encrypting, by at least one machine in a set of one or more machines, the digital message using a recipient public key RPUB and a recipient encryption key RENC to create an encrypted digital message for decryption with a recipient private key RPRIV and a recipient decryption key RDEC, wherein:

a key formed from the recipient encryption key RENC and a key formed from the recipient decryption key RDEC are a public key/ private key pair 1;

the recipient public key RPUB and the recipient private key RPRIV form a public key/private key pair 2, wherein the recipient private key RPRIV is a secret of the recipient;

the recipient encryption key RENC is generated using identity information of at least one of the recipient's ancestors;

the recipient decryption key RDEC is generated such that the recipient decryption key RDEC is related to the recipient encryption key RENC, a root key generation secret and an associated root key generation parameter, wherein the root key generation parameter is generated based on the root key generation secret, and the root key generation secret is a secret of the root authorizer.

19. (currently amended) The method of claim 18, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient.

20. (currently amended) The method of claim 18, wherein the recipient encryption key RENC is generated from information comprising a parameter defining a validity period for the recipient decryption key RDEC.

21. (currently amended) The method of claim 18, wherein the recipient encryption key RENC is generated from information comprising the recipient public key RPUB.

22. (currently amended) The method of claim 18, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient, the recipient public key RPUB, and a parameter defining a validity period for the recipient decryption key RDEC.

23. (currently amended) The method of claim 18, wherein the recipient decryption key RDEC is generated according to a schedule known to the sender.

24. (currently amended) The method of claim 18, wherein the recipient private key RPRIV and the recipient public key RPUB are generated using system parameters issued by one or more of the authorizers.

25. (currently amended) The method of claim 18, wherein the recipient decryption key RDEC is related to the root key generation secret and the associated root key generation parameter.

26. (currently amended) The method of claim 18, wherein the plurality of authorizers further includes at least m lower-level authorizers in the hierarchy between the root authorizer and the sender, wherein $m \geq 1$, and wherein l of the m authorizers in the hierarchy are common ancestors to both the sender and the recipient, wherein authorizer is the lowest common ancestor authorizer between the sender and the recipient, and wherein $l \geq 1$, and wherein:

a lower-level key generation secret is selected for each of the m lower-level authorizers in the hierarchy between the root authorizer and the sender; and

a sender decryption key SDEC is generated such that the sender decryption key SDEC is related to at least the root key generation secret and one or more of the m lower-level key generation secrets associated with the m lower-level authorizers in the hierarchy between the root authorizer and the sender;

wherein the message is encrypted using at least the sender decryption key SDEC and one or more of the lower-level key generation parameters associated with the $(m - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers above the lowest common ancestor authorizer$_l$; and

wherein the encrypted digital message is decryptable using at least the recipient decryption key RDEC and one or more of the lower-level key generation parameters associated with the $(n - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers that above the lowest common ancestor authorizer$_l$.

27-116. (cancelled)

117. (currently amended) The method of claim 1 wherein the method further comprises the recipient performing, by at least one machine in the set of the one or more machines, operations of:

generating the recipient public key RPUB and the recipient private key RPRIV;

decrypting the encrypted digital message using at least the recipient private key RPRIV and the recipient decryption key RDEC.

118. (currently amended) The method of claim 1 wherein the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating the recipient decryption key RDEC and sending the recipient decryption key to the recipient.

119. (canceled)

120. (currently amended) The method of claim 118 wherein the method further comprises the recipient performing, by at least one machine in the set of the one or more machines, operations of:

generating the recipient public key RPUB and the recipient private key RPRIV;

decrypting the encrypted digital message using at least the recipient private key RPRIV and the recipient decryption key RDEC.

121-123. (canceled)

124. (currently amended) The method of claim 1 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC by the authorizer and/or the recipient and/or the sender.

125. (currently amended) The method of claim 2 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

126. (currently amended) The method of claim 3 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

127. (currently amended) The method of claim 4 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

128. (currently amended) The method of claim 5 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

129. (currently amended) The method of claim 6 wherein the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC and sending, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC to the recipient.

130. (currently amended) The method of claim 7 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

131. (currently amended) The method of claim 9 wherein the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC and sending, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC to the recipient.

132. (currently amended) The method of claim 10 wherein the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC and sending, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC to the recipient.

133. (currently amended) The method of claim 11 wherein the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC and sending, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC to the recipient.

134. (currently amended) The method of claim 12 wherein the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC and sending, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC to the recipient.

135. (currently amended) The method of claim 13 wherein the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC and sending, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC to the recipient.

136. (currently amended) The method of claim 14 wherein the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC and sending, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC to the recipient.

137. (canceled)

138. (currently amended) The method of claim 16 wherein the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC and sending, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC to the recipient.

139. (currently amended) The method of claim 16 wherein the method further comprises the recipient performing, by at least one machine in the set of the one or more machines, operations of:

generating the recipient public key RPUB and the recipient private key RPRIV;

decrypting the encrypted digital message using at least the recipient private key RPRIV and the recipient decryption key RDEC.

140. (canceled)

141. (currently amended) The method of claim 18 wherein the method further comprises the recipient performing, by at least one machine in the set of the one or more machines, operations of.

generating the recipient public key RPUB and the recipient private key RPRIV; and

decrypting the encrypted digital message to recover the digital message using at least the recipient private key RPRIV and the recipient decryption key RDEC.

142. (previously presented) The method of claim 18 wherein the method further comprises the root authorizer performing, by at least one machine in the set of the one or more machines, operations of:

selecting the root key generation secret that is a secret of the root authorizer; and

generating the root key generation parameter based on the root key generation secret.

143. (currently amended) The method of claim 18 wherein the method further comprises generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC by one of the authorizers.

144. (canceled)

145. (currently amended) The method of claim 142 wherein further comprising the recipient performing, by at least one machine in the set of the one or more machines, operations of.

generating the recipient public key RPUB and the recipient private key RPRIV; and

decrypting the encrypted digital message to recover the digital message using at least the recipient private key RPRIV and the recipient decryption key RDEC.

146-148. (canceled)

149. (currently amended) The method of claim 18 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

150. (currently amended) The method of claim 19 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

151. (currently amended) The method of claim 20 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

152. (currently amended) The method of claim 21 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

153. (currently amended) The method of claim 22 further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key RENC.

154. (currently amended) The method of claim 23 wherein the method further comprises generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC by one of the authorizers.

155. (currently amended) The method of claim 25 wherein the method further comprises generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC by one of the authorizers.

156. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 1.

157. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 5.

158. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 9.

159. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 10.

160. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 11.

161. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 13.

162. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 15.

163. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 16.

164. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 17.

165. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 18.

166. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 20.

167. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 22.

168. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 23.

169. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 26.

170. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 117.

171. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 118.

172. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim [[119]] 120.

173. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim [[123]] 124.

174. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 127.

175. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 130.

176. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 136.

177. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim [[140]] 139.

178. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 141.

179. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 142.

180. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 143.

181. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim [[147]] 149.

182. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 150.

183. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 152.

184. (currently amended) A method for operating a public-key encryption scheme which provides for sending a digital message M between a sender and a recipient with participation of an authorizer, wherein the digital message M is encrypted by the sender using at least a recipient public key RPUB and a recipient encryption key RENC to create an encrypted digital message and is decrypted by the recipient, the method comprising decrypting, by at least one machine in a set of one or more machines, the encrypted digital message using at least a recipient private key RPRIV and a recipient decryption key RDEC, wherein:

the recipient public key RPUB and the recipient private key RPRIV form a public key/ private key pair 1, wherein the recipient private key RPRIV is a secret of the recipient;

the recipient decryption key RDEC is generated using at least a key generation secret of the authorizer and the recipient encryption key RENC, wherein a key formed from the recipient encryption key RENC and a key formed from the recipient decryption key RDEC are a public key/ private key pair 2.

185. (currently amended) The method of claim 184, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient.

186. (currently amended) The method of claim 184, wherein the recipient encryption key RENC is generated from information comprising a parameter defining a validity period for the recipient decryption key RDEC.

187. (currently amended) The method of claim 184, wherein the recipient encryption key RENC is generated from information comprising the recipient public key RPUB.

188. (currently amended) The method of claim 184, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient, the recipient public key RPUB, and a parameter defining a validity period for the recipient decryption key RDEC.

189. (currently amended) The method of claim 184, wherein the recipient decryption key RDEC is generated by the authorizer according to a schedule known to the sender.

190. (currently amended) The method of claim 189, wherein the recipient encryption key RENC is generated using at least information comprising the schedule.

191. (currently amended) The method of claim 184, wherein the recipient private key RPRIV and the recipient public key RPUB are generated using at least one system parameter issued by the authorizer.

192. (currently amended) The method of claim 184, wherein the recipient decryption key RDEC is generated by the authorizer to have a value $S = s_c P_B$, wherein:

s_c is the key generation secret of the authorizer; and

P_B is the recipient encryption key RENC and is equal to $H_1(\text{Inf}_B)$, wherein Inf_B is an element of a first cyclic group $\mathbb{G}_1$ of elements, wherein P_B is an element of a second cyclic group $\mathbb{G}_2$ of elements, and H_1 is a predefined function ("first function H_1"), wherein the first and second cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ and the function H_1 are system parameters made available to the sender, and also available to the sender are system parameters comprising:

a generator P of the first cyclic group $\mathbb{G}_1$;

a key generation parameter $Q = s_C P$;

a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$.

193. (currently amended) The method of claim 192, wherein Inf_B comprises the identity of the recipient, ID_{rec}, the recipient public key RPUB, and a parameter defining a validity period for the recipient decryption key RDEC.

194. (previously presented) The method of claim 192, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

195. (previously presented) The method of claim 192 wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

196. (previously presented) The method of claim 192 wherein the system parameters available to the sender further comprise a function $\hat{e}$ which is a bilinear, non-degenerate, and efficiently computable pairing which maps $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$.

197. (previously presented) The method of claim 194 wherein:

s_C is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$.

198. (currently amended) The method of claim 192, wherein encrypting the digital message M comprises:

generating an element $P'_B = H_1(ID_{rec})$, wherein ID_{rec} comprises the identity of the recipient and wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

selecting a random key generation secret r; and

encrypting the digital message M to form a ciphertext C, wherein C is set to be:

$C = [rP, M \oplus H_2(g^r)]$, where $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, where PK_B is the recipient public key RPUB and wherein $\hat{e}$ is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$.

199. (currently amended) The method of claim 184, wherein the recipient encryption key RENC is generated from a document and the recipient decryption key RDEC is the authorizer's signature on the document.

200. (currently amended) The method of claim 194, wherein encrypting the digital message M comprises:

generating an element $P'_B = H_1(ID_{rec})$ wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

choosing a random parameter $\sigma \in \{0,1\}^n$;

set a random key generation secret $r = H_3(\sigma, M)$; and

encrypting the digital message M to form a ciphertext C, wherein C is set to be:

$C = [rP, M \oplus H_2(g^r), E_{H_4(\sigma)}(M)]$, where $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, wherein PK_B is the recipient public key RPUB, wherein H_3 is a function capable of generating an integer of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ from two strings of binary digits, H_4 is a function capable of generating one binary string from another binary string, E is a symmetric encryption scheme, $\hat{e}$ is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$, and $H_4(\sigma)$ is the key used with E.

201. (currently amended) The method of claim 184 further comprising the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC and sending, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC to the recipient.

202. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 184.

203. (currently amended) A method for operating a public-key encryption scheme which provides for sending a digital message M between a sender and a recipient with participation of an authorizer, wherein the digital message is encrypted by the sender using at least a recipient public key RPUB and a recipient encryption key RENC, wherein the recipient public key RPUB and a recipient private key RPRIV form a recipient public key/ recipient private key pair, wherein the recipient private key RPRIV is a secret of the recipient, and the digital message is decrypted by the recipient using at least the recipient private key RPRIV and a recipient decryption key RDEC, the method comprising the authorizer performing, by at least one machine in a set of one or more machines, operations of:

selecting a key generation secret that is a secret of the authorizer;

generating [[a]] the recipient decryption key RDEC using at least the key generation secret of the authorizer and the recipient encryption key RENC, wherein a key formed from the recipient encryption key RENC and a key formed from the recipient decryption key RDEC are a public key/ private key pair;

sending the recipient decryption key RDEC to the recipient.

204. (currently amended) The method of claim 203, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient.

205. (currently amended) The method of claim 203, wherein the recipient encryption key RENC is generated from information comprising a parameter defining a validity period for the recipient decryption key RDEC.

206. (currently amended) The method of claim 203, wherein the recipient encryption key RENC is generated from information comprising the recipient public key RPUB.

207. (currently amended) The method of claim 203, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient, the recipient public key RPUB, and a parameter defining a validity period for the recipient decryption key RDEC.

208. (currently amended) The method of claim 203, wherein the recipient decryption key RDEC is generated by the authorizer according to a schedule known to the sender.

209. (currently amended) The method of claim 208, wherein the recipient encryption key RENC is generated using at least information comprising the schedule.

210. (currently amended) The method of claim 203, wherein the recipient decryption key RDEC is generated by the authorizer to have a value $S = s_c P_B$, wherein:

s_c is the key generation secret of the authorizer; and

P_B is the recipient encryption key RENC and is equal to $H_1(\text{Inf}_B)$, wherein Inf_B is an element of a first cyclic group $\mathbb{G}_1$ of elements, wherein P_B is an element of a second cyclic group $\mathbb{G}_2$ of elements, and H_1 is a predefined function ("first function H_1"), wherein the first and second cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ and the function H_1 are system parameters made available to the sender, and also available to the sender are system parameters comprising:

a generator P of the first cyclic group $\mathbb{G}_1$;

a key generation parameter $Q = s_C P$;

a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$.

211. (currently amended) The method of claim 210, wherein Inf_B comprises the identity of the recipient, ID_{rec}, the recipient public key RPUB, and a parameter defining a validity period for the recipient decryption key RDEC.

212. (previously presented) The method of claim 210, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

213. (previously presented) The method of claim 210 wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

214. (previously presented) The method of claim 210 wherein the system parameters available to the sender further comprise a function $\hat{e}$ which is a bilinear, non-degenerate, and efficiently computable pairing which maps $\mathbb{G}_1 \text{ X } \mathbb{G}_1$ into $\mathbb{G}_2$.

215. (previously presented) The method of claim 212 wherein:

s_C is an element of the cyclic group $\mathbb{Z} / q\mathbb{Z}$.

216. (currently amended) The method of claim 203, wherein the recipient encryption key RENC is generated from a document and the recipient decryption key RDEC is the authorizer's signature on the document.

217. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 203.

218. (currently amended) A method for operating a public-key encryption scheme which provides for sending a digital message between a sender and a recipient with participation of a plurality of authorizers, the plurality of authorizers including a root authorizer and n lower-level authorizers in a hierarchy between the root authorizer and the recipient, wherein $n \geq 1$, wherein the digital message is encrypted by the sender using a recipient public key RPUB and a recipient encryption key RENC to create an encrypted digital message for decryption by the recipient using a recipient private key RPRIV and a recipient decryption key RDEC,

the method comprising performing, by at least one machine in a set of one or more machines, operations of:

generating the recipient public key RPUB and the recipient private key RPRIV which are a public key/private key pair 1, wherein the recipient private key RPRIV is a secret of the recipient;

obtaining an encrypted digital message formed by encryption of the digital message with the recipient public key RPUB and the recipient encryption key RENC, wherein a key formed from the recipient encryption key RENC and a key formed from the recipient decryption key RDEC are a public key/ private key pair 2; and

decrypting the encrypted digital message to recover the digital message using at least the recipient private key RPRIV and the recipient decryption key RDEC;

wherein the recipient encryption key RENC is generated using identity information of at least one of the recipient's ancestors;

wherein the recipient decryption key RDEC is generated such that the recipient decryption key RDEC is related to the recipient encryption key RENC, a root key generation secret and an associated root key generation parameter, wherein the root key generation parameter is generated based on the root key generation secret, and the root key generation secret is a secret of the root authorizer.

219. (currently amended) The method of claim 218, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient.

220. (currently amended) The method of claim 218, wherein the recipient encryption key RENC is generated from information comprising a parameter defining a validity period for the recipient decryption key RDEC.

221. (currently amended) The method of claim 218, wherein the recipient encryption key RENC is generated from information comprising the recipient public key RPUB.

222. (currently amended) The method of claim 218, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient, the recipient public key RPUB, and a parameter defining a validity period for the recipient decryption key RDEC.

223. (currently amended) The method of claim 218, wherein the recipient decryption key RDEC is generated according to a schedule known to the sender.

224. (currently amended) The method of claim 218, wherein the recipient private key RPRIV and the recipient public key RPUB are generated using system parameters issued by one or more of the authorizers.

225. (currently amended) The method of claim 218, wherein the recipient decryption key RDEC is related to the root key generation secret and the associated root key generation parameter.

226. (currently amended) The method of claim 218, wherein the plurality of authorizers further includes at least m lower-level authorizers in the hierarchy between the root authorizer and the sender, wherein $m \geq 1$, and wherein l of the m authorizers in the hierarchy are common ancestors to both the sender and the recipient, wherein authorizer is the lowest common ancestor authorizer between the sender and the recipient, and wherein $l \geq 1$, and wherein:

a lower-level key generation secret is selected for each of the m lower-level authorizers in the hierarchy between the root authorizer and the sender; and

a sender decryption key SDEC is generated such that the sender decryption key SDEC is related to at least the root key generation secret and one or more of the m lower-level key generation secrets associated with the m lower-level authorizers in the hierarchy between the root authorizer and the sender;

wherein the message is encrypted using at least the sender decryption key SDEC and one or more of the lower-level key generation parameters associated with the $(m - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers above the lowest common ancestor authorizer$_l$; and

wherein the encrypted digital message is decryptable using at least the recipient decryption key RDEC and one or more of the lower-level key generation parameters associated with the $(n - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers that above the lowest common ancestor authorizer$_l$.

227. (currently amended) The method of claim 218 further comprising generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC by one of the authorizers.

228. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 218.

229. (currently amended) A method for operating a public-key encryption scheme which provides for sending a digital message between a sender and a recipient with

participation of a plurality of authorizers, the plurality of authorizers including a root authorizer and n lower-level authorizers in a hierarchy between the root authorizer and the recipient, wherein $n \geq 1$, wherein the digital message is encrypted by the sender using a recipient public key RPUB and a recipient encryption key RENC to create an encrypted digital message for decryption by the recipient using a recipient private key RPRIV and a recipient decryption key RDEC,

the method comprising generating, by at least one machine in a set of one or more machines, the recipient decryption key RDEC such that the recipient decryption key RDEC is related to the recipient encryption key RENC, a root key generation secret and an associated root key generation parameter, wherein the root key generation parameter is generated based on the root key generation secret, and the root key generation secret is a secret of the root authorizer;

wherein the recipient encryption key RENC is generated using identity information of at least one of the recipient's ancestors;

wherein a key formed from the recipient encryption key RENC and a key formed from the recipient decryption key RDEC are a public key/ private key pair 1;

wherein the recipient public key RPUB and the recipient private key RPRIV are a public key/private key pair 2, wherein the recipient private key RPRIV is a secret of the recipient.

230. (currently amended) The method of claim 229, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient.

231. (currently amended) The method of claim 229, wherein the recipient encryption key RENC is generated from information comprising a parameter defining a validity period for the recipient decryption key RDEC.

232. (currently amended) The method of claim 229, wherein the recipient encryption key RENC is generated from information comprising the recipient public key RPUB.

233. (currently amended) The method of claim 229, wherein the recipient encryption key RENC is generated from information comprising the identity of the recipient,

the recipient public key RPUB, and a parameter defining a validity period for the recipient decryption key RDEC.

234. (currently amended) The method of claim 229, wherein the recipient decryption key RDEC is generated according to a schedule known to the sender.

235. (currently amended) The method of claim 229, wherein the recipient private key RPRIV and the recipient public key RPUB are generated using system parameters issued by one or more of the authorizers.

236. (currently amended) The method of claim 229, wherein the recipient decryption key RDEC is related to the root key generation secret and the associated root key generation parameter.

237. (currently amended) The method of claim 229, wherein the plurality of authorizers further includes at least m lower-level authorizers in the hierarchy between the root authorizer and the sender, wherein $m \geq 1$, and wherein l of the m authorizers in the hierarchy are common ancestors to both the sender and the recipient, wherein authorizer is the lowest common ancestor authorizer between the sender and the recipient, and wherein $l \geq 1$, and wherein:

a lower-level key generation secret is selected for each of the m lower-level authorizers in the hierarchy between the root authorizer and the sender; and

a sender decryption key SDEC is generated such that the sender decryption key SDEC is related to at least the root key generation secret and one or more of the m lower-level key generation secrets associated with the m lower-level authorizers in the hierarchy between the root authorizer and the sender;

wherein the message is encrypted using at least the sender decryption key SDEC and one or more of the lower-level key generation parameters associated with the $(m - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation

parameters that are associated with the (l - 1) authorizers above the lowest common ancestor authorizer$_l$; and

wherein the encrypted digital message is decryptable using at least the recipient decryption key RDEC and one or more of the lower-level key generation parameters associated with the ($n - l + 1$) authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the (l - 1) authorizers that above the lowest common ancestor authorizer$_l$.

238. (currently amended) The method of claim 229 further comprising generating, by at least one machine in the set of the one or more machines, the recipient decryption key RDEC by one of the authorizers.

239. (previously presented) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 229.